Amendments to the Claims

1. (currently amended) A system for authenticating an encryption key of a user at a remote computer remotely networked to a server computer, comprising: a decrypt engine in the remote computer for using a password provided by the user to decrypt in the remote computer an encrypted data file provided by the user ~~into~~ so as to form a decrypted data file and so as to use the decrypted data file to form at least part of the encryption key of the user, without transmitting to the server either the password, the encrypted data file or the decrypted data file.

2. (previously amended) The system of claim 1, wherein the encrypted data file is stored on an RF smart card.

3. (previously amended) The system of claim 1, wherein the encrypted data file includes encrypted biometric data identifying the user.

4. (cancelled).

5. (cancelled)

6. (cancelled)

7. (currently amended) A method for providing an authenticated encryption key of a user at a remote computer remotely networked to a server computer, comprising the steps of:

providing an encrypted data file to the remote computer;

providing a password to the remote computer; and

decrypting the encrypted data file in the remote computer using the password so as to generate an authenticated encryption key of the user without transmitting to the server either the password or, the encrypted data file.

8. (previously amended) The method of claim 7, wherein the encrypted data file is stored on an RF smart card.

9. (previously amended) The method of claim 7, wherein th encrypted data file includes encrypted biometric data identifying the user.

10. (original) The method of claim 9, wherein the biometric data includes a digitized fingerprint of the user.

11. (previously amended) The method of claim 7, further including the steps of:

generating biometric data of the user by scanning a biometric feature of the user; and

probabilistically comparing the generated biometric data of the user to data derived from the encrypted data file to authenticate the encryption key of the user.

12. (original) The method of claim 11, wherein the scanned biometric feature of the user is a fingerprint.

13. (currently amended) A computer-accessible medium comprising program instructions for providing at a remote computer remotely networked to a server computer an authenticated encryption key of a user, comprising the steps of:

using a password provided by the user to decrypt in the remote computer an encrypted data file provided by the user so as to form a decrypted data file and so as to use the decrypted data file to form at least part of~~into~~ an authenticated encryption key of the user without transmitting to the server either the password, the encrypted data file or the decrypted data file.

14. (Previously added) The system of claim 1, wherein the encrypted data file includes encrypted biometric data, derived from a digitized fingerprint of the user, identifying the user.

15. (Previously added) The system of claim 1, further comprising a biometric reader for generating a first biometric data of the user, wherein the first biometric data of the user is compared with a second biometric data of the user stored in the encrypted data file.

16. ((Previously added) The system of claim 1, further comprising a fingerprint scanner for generating a first digitized fingerprint of the user, wherein the first digitized fingerprint of the user is compared with a second digitized fingerprint of the user stored in the encrypted data file.

17. (Currently amended) A system for authenticating an encryption key of a user, comprising:

an input device at a remote computer remotely networked to a server computer for receiving a password provided by the user at the remote computer remotely networked to a server computer;

memory in the remote computer for storing an encrypted data file including an encryption key of the user; and

a decrypt engine in the remote computer for using the password to decrypt the encrypted data file ~~and thereby generating~~so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer an authenticated encryption key of the user, without transmitting to the server either the password, the encrypted data file or the decrypted data file.

18. (Previously added) The system of claim 17, wherein the encrypted data file is stored on an RF smart card.

19. (Previously added) The system of claim 17, wherein the encrypted data file includes encrypted biometric data identifying the user.

20. (Previously added) The system of claim 17, wherein the encrypted data file includes encrypted biometric data, derived from a digitized fingerprint of the user, identifying the user.

21. (Previously added) The system of claim 17, further comprising a biometric reader for generating a first biometric data of the user, wherein the first biometric data of the user is compared with a second biometric data of the user stored in the encrypted data file.

22. (Previously added) The system of claim 17, further comprising a fingerprint scanner for generating a first digitized fingerprint of the user, wherein the first digitized fingerprint of the user is compared with a second digitized fingerprint of the user stored in the encrypted data file.

23. (Previously added) The system of claim 17, further comprising a server configured to receive data encrypted using the authenticated encryption key.

24. (Currently amended) A system for authenticating an encryption key of a user at a remote computer remotely networked to a server computer, comprising:

an input device at the remote computer for receiving a password provided by the user;

an RF smart card for storing an encrypted data file, the encrypted data file including an encryption key of the user;

a decrypt engine in the remote computer for using the password to decrypt the encrypted data file so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer ~~and thereby generate~~ an authenticated encryption key of the user without transmitting to the server either the password, the encrypted data file, or the decrypted data file; and

memory in the remote computer for storing the decrypt engine.

25. (Previously added) The system of claim 24, wherein the encrypted data file includes encrypted biometric data identifying the user.

26. (Previously added) The system of claim 24, wherein the encrypted data file includes encrypted biometric data, derived from a digitized fingerprint of the user, identifying the user.

27. (Currently amended) A system for authenticating an encryption key of a user at a remote computer remotely networked to a server computer, comprising:

an input device at the remote computer for receiving a password provided by the user;

an RF smart card for storing an encrypted data file, the encrypted data file including an encryption key of the user and ~~a~~ first biometric data of the user;

a biometric reader for generating ~~a~~ second biometric data of the user; and

a decrypt engine in the remote computer for using the password to decrypt the encrypted data file, so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer ~~thereby generating~~ an authenticated encryption key of the user, if there is a probabilistic match between the first biometric data and the second biometric data without transmitting to the server either the password, the encrypted data file or the decrypted data file.

28. (Currently amended) A system for authenticating an encryption key of a user at a remote computer remotely networked to a server computer, comprising:

memory in the remote computer for storing an encrypted encryption key;

an input device at the remote computer for receiving a password;

a decrypt engine in the remote computer for using the password to decrypt the encrypted encryption key so as to form an authenticated decrypted encryption key without transmitting to the server either the password, the encrypted data file or the decrypted data file; and

memory in the remote computer for storing the decrypt engine without transmitting to the server either the password, the encrypted data file or the decrypted data file.

29. (Previously added) The system of claim 28, wherein the encrypted data file includes encrypted biometric data identifying the user.

30. (Previously added) The system of claim 28, wherein the encrypted encryption key in is stored on an RF smart card.

31. (Currently amended) A system for authenticating an encryption key of a user at a remote computer remotely networked to a server computer, comprising:

memory in the remote computer for storing an encrypted encryption key and a first biometric data of the user;

an input device at the remote computer for receiving a password;

a biometric reader at the remote computer for generating a second biometric data of the user;

a decrypt engine in the remote computer for comparing the first biometric data of the user with a second biometric data of the user and, if there is a probabilistic match, then using the password to decrypt the encrypted encryption key so as to form an authenticated decrypted encryption key without transmitting to the server either the password, or the encrypted encryption key; and

memory in the remote computer for storing the decrypt engine without transmitting to the server either the password, or the encrypted encryption key.

32. (Previously added) The system of claim 31, wherein the password is used to decrypt the first biometric data before comparison with the second biometric data.

33. (Previously added) The system of claim 31, wherein the biometric reader is a fingerprint scanner for generating a first digitized fingerprint of the user, and the first biometric data is a digitized fingerprint of the user.

34. (Currently amended) A method for authenticating an encryption key of a user at a remote computer remotely networked to a server computer, comprising the steps of:

storing an encrypted encryption key in memory in a remote computer;

receiving a password provided by a user; and

requiring use of the password in the remote computer to decrypt the encrypted encryption key so as to form a decrypted encrypting key without transmitting to the server either the password, or the encrypted encryption key.

35. (Currently amended) The method of claim 34, wherein the encrypted encryption key is stored on an ~~a~~ RF smart card.

36. (Previously added) The method of claim 34, wherein the encrypted encryption key is stored with encrypted biometric data identifying the user.

37. (Previously added) The method of claim 36, wherein the encrypted biometric data includes a digitized fingerprint of the user.

38. (Previously added) The system of claim 36, wherein the password is used to decrypt the first biometric data before comparison with the second biometric data.

39. (Currently amended) The method of claim 34, further comprising the steps of:

scanning a biometric feature of the user to generate first biometric data of the user;

decrypting second biometric data stored along with the encrypted encryption key;~~.~~

probabilistically comparing the generated first biometric data to the decrypted second biometric data; and

requiring the comparison to produce a probabilistic match before decrypting the encrypted encryption key to the decrypted encryption key.

40. (Previously added) The method of claim 32, further comprising the step of reading the encrypted encryption key from an RF smart card.

41. (Previously added) The method of claim 32, further comprising the step of using the decrypted encryption key to encrypt data.

42. (New) A system for authenticating an encryption key of a user at a remote computer remotely networked to a server computer and transmitting secure data to the server computer, the system comprising:

a remote password receiving and processing means for receiving a password from a user and authenticating the password to provide an authenticated password at the remote computer

means at the remote computer and isolated from the server computer for receiving the authenticated password, for receiving an encrypted first data file from the user, and for generating a decryption key at the remote computer for decrypting the encrypted first data file at the remote computer, and means for decrypting the encrypted first data file to form a decrypted first data file at the remote computer,

means for generating an encryption key at the remote computer using the decrypted first data file, for encrypting a second date file at the remote computer to form an encrypted second data file for transmission to the server using the encryption key, and for transmitting the encrypted second data file to the server without transmitting to the server either the password, the authenticated password, the encrypted first data file, the decrypted first data file, or the encryption key.

PAGE 16/19 * RCVD AT 5/27/2004 5:01:11 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:250 861 8772 * DURATION (mm-ss):05-52